

Item. 2

**Family list**

2 family members for:

**JP8305662**

Derived from 2 applications.

**1 METHOD AND SYSTEM FOR CLIENT AUTHENTICATION**

Publication info: **JP8305662 A** - 1996-11-22

**2 System for and method of authenticating a client**

Publication info: **US5784464 A** - 1998-07-21

---

Data supplied from the *esp@cenet* database - Worldwide

(43)公開日 平成8年(1996)11月22日

(51) Int.Cl. <sup>5</sup>		識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F	15/00	3 3 0	9364-5L	G 0 6 F 15/00	3 3 0 C
	13/00	3 5 1	7368-5E	13/00	3 5 1 E

審査請求 未請求 請求項の数9 OL (全 22 頁)

(21)出願番号	特願平7-108408	(71)出願人	000005223 富士通株式会社 神奈川県川崎市中原区上小田中4丁目1番1号
(22)出願日	平成7年(1995)5月2日	(72)発明者	秋山 良太 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(72)発明者	宗像 昭夫 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(74)代理人	弁理士 遠山 勉 (外1名)

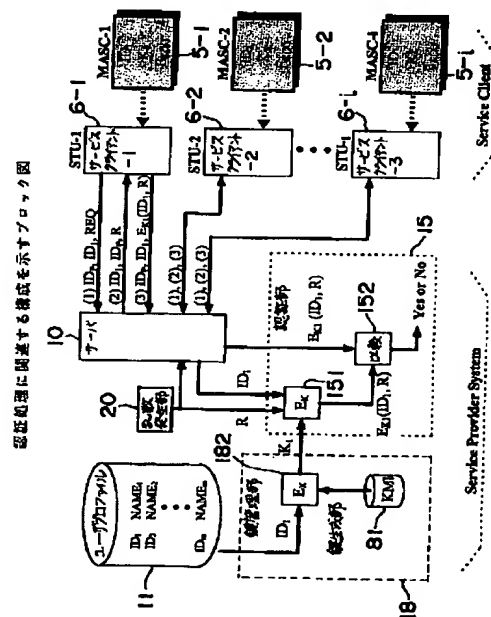
最終頁に続く

(54) 【発明の名称】 クライアント認証システムおよび方法

(57) 【要約】

【目的】クライアントとサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方において動的に作成することにより、これらの第三者による盗用が不可能となるクライアント認証システムを提供する。

【構成】サービス提供者側システム１の鍵管理部１８は、アクセス要求を行ったサービスクライアント６に接続されたＭＡＳＣ５に対応する個別鍵Ｋを生成し、この個別鍵Ｋを認証部１５に通知する。この個別鍵は、予め、ＭＡＳＣ５にも格納されている。乱数発生器２０は、乱数Ｒを生成して、ＭＡＳＣ５に送信するとともに、認証部１５に通知する。ＭＡＳＣ５は、この乱数を個別鍵によって暗号化して、サービス提供者側システム１に戻す。一方、認証部１５の暗号化部１５１は、乱数Ｒを個別鍵Ｋによって暗号化する。そして、認証部１５の比較器１５２は、暗号化部１５１が暗号化したデータとＭＡＳＣ５から送信されてきた暗号化データを比較して、両者が一致した場合には、このＭＡＳＣ５からのアクセス要求であると確認する。



## 【特許請求の範囲】

【請求項1】データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して配送されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証システムにおいて、前記データ供給装置は、前記クライアントに対応する第1の鍵を出力する鍵出力部と、前記クライアントからのアクセス要求に応じて乱数を生ずる乱数発生手段と、前記鍵出力部において出力された第1の鍵によって前記乱数を暗号化することによって第1の認証子を出力する第1の暗号化手段と、前記クライアントに前記乱数を送信する第1の送信手段と、前記クライアントから第2の認証子を受信する第1の受信手段と、前記第1の認証子と前記第2の認証子とを比較して両者が一致している場合に当該クライアントからのアクセス要求であると認証する比較手段とを備え、前記クライアントは、前記データ供給装置にアクセス要求を行うアクセス要求手段と、前記データ供給装置から送信された前記乱数を受信する第2の受信手段と、前記第1の鍵と同一の第2の鍵を保持する鍵保持手段と、前記第2の鍵によって前記乱数を暗号化することによって前記第2の認証子を出力する第2の暗号化手段と、前記データ供給装置に前記第2の認証子を送信する第2の送信手段とを備えることを特徴とするクライアント認証システム。

【請求項2】前記アクセス要求手段は、前記アクセス要求に際してそのクライアントに設定された固有の識別情報を前記データ供給装置に通知するとともに、前記鍵出力部は、各クライアントに固有の前記識別情報を加工することにより前記第1の鍵を生成することを特徴とする請求項1記載のクライアント認証システム。

【請求項3】前記データ供給装置は前記比較手段によって前記両認証子が一致すると判断された場合のみ前記データを前記クライアントに配送することを特徴とする請求項1記載のクライアント認証システム。

【請求項4】前記データ供給装置は暗号化された前記データを前記クライアントに配送するとともに、前記クライアントは前記暗号化された前記データを復号化する第1の復号化手段を備えることを特徴とする請求項1記載のクライアント認証システム。

【請求項5】前記データ供給装置は前記データを復号化するための第3の鍵を前記第1の鍵によって暗号化する第3の暗号化手段を備えているとともに、

前記クライアントは前記暗号化された前記第3の鍵を前記第2の鍵によって復号化する第2の復号化手段を備え、前記第1の復号化手段はこの第2の復号化手段によって復号化された前記第3の鍵によって前記暗号化されたデータを復元することを特徴とする請求項4記載のクライアント認証システム。

【請求項6】前記データ供給装置は、前記暗号化されたデータを格納するための複数の格納装置を備えるとともに、一方の格納装置に格納されている前記暗号化されたデータを前記第3の鍵を用いて復号化する第3の復号化手段と、第3の鍵を更新する鍵更新手段と、第3の復号化手段によって復号化されたデータを前記鍵更新手段によって更新された前記第3の鍵によって暗号化する第3の暗号化手段と、

第3の暗号化手段によって暗号化されたデータを他の前記格納装置に格納する書込手段とを更に備えたことを特徴とする請求項5記載のクライアント認証システム。

【請求項7】前記第3の復号化手段、前記鍵更新手段、前記第3の暗号化手段、及び前記書込手段は一定時間毎に起動することを特徴とする請求項6記載のクライアント認証システム。

【請求項8】前記クライアントは、前記データを受信する本体部とこの本体部に対して着脱自在に設けられたモジュール部とから構成されるときともに、少なくとも前記鍵保持手段及び前記第2の暗号化手段は前記モジュール部に備えられていることを特徴とする請求項1記載のクライアント認証システム。

【請求項9】データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して送出されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証方法において、前記クライアントは自己を識別する識別情報を付して前記データ供給装置にアクセス要求を行い、前記データ供給装置は、このアクセス要求に応じて乱数を生ずるしてこの乱数を前記クライアントに送出するとともに、前記識別情報に対応する第1の鍵によって前記乱数を暗号化して第1の認証子に変換し、前記クライアントは前記第1の鍵と同一内容を有するものとして予め保持している第2の鍵によって前記乱数を暗号化して第2の認証子に変換するとともに、この第2の認証子を前記データ供給装置に送出し、前記データ供給装置は前記第1の認証子と前記第2の認証子とを比較して両者が一致した場合に前記クライアントからのアクセス要求があったことを認証することを特徴とするクライアント認証方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、クライアントからの要求に応じて、映像著作物等のソフトウェアを通信手段を介して配送するシステム（デジタル・オーディオ・インタラクティブ・システム）におけるクライアント認証システム及び認証方法に関する。

【0002】

【従来の技術】近年、ケーブルテレビジョンシステムや通信衛星を用いた通信システムの構築を背景に、デジタル情報化されたソフトウェア（音声データ、映像データ等、以下、「コンテンツ」という）を各家庭等に配送するサービスが提案されている。このサービスシステムは、ビデオ・オン・デマンド方式等と呼ばれるデジタル・オーディオ・インタラクティブ・システムである。このデジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者とユーザとの間で電話線等を介した通信が行われる。そして、サービス提供者は、ユーザから要求された時刻に要求された内容のコンテンツをこのユーザに配送するとともに、このソフトウェアの使用料金をクレジットカード会社等を通じて当該ユーザに課金し、その一部をコンテンツ供給者に還元するのである。

【0003】このようなデジタル・オーディオ・インタラクティブ・システムが普及してゆく上で重要な事は、インフラストラクチャーとなるサーバ/ネットワーク/ターミナルが低コストで構築されることは勿論であるが、これらを媒介としてユーザに提供されるコンテンツが豊富に準備されなければ、成功とはならないということである。即ち、コンテンツとインフラストラクチャーは車の両輪であるので、コンテンツ提供者がコンテンツ提供による利益回収を見込めるとともに不測の損害を被る危険がない仕組みをこのインフラストラクチャーに組み込むことにより、コンテンツが集まりやすい環境を整備することが不可欠なのである。なお、このような仕組みは、コンテンツ提供者とユーザとを媒介する供給メディアの種類（広帯域ケーブルネットワーク、衛星システム、移動通信、光メディアパッケージ等）に拘わらず、整備されていなければならない。

【0004】このような環境の整備がなされることにより、コンテンツ供給者は、安心して気軽に、コンテンツを供給することができるようになる。一方、ユーザは、いつでもどこでも、簡単な手続きによって必要なコンテンツを手に入れることができるようになる。このことが、システムをより一層普及させるために重要なポイントとなっているのである。

【0005】一方、システム構築に当たっては、誰もが参加できるオープン性が重要であり、既存の標準技術を可能な限り活用する方式を取っていくことが必要である。また、技術の進歩や各種サービスの多様化に対応できる拡張性も持ち合わせたものであることを併せて考慮すべきである。

【0006】

【発明が解決しようとする課題】以上説明したように、デジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者は、コンテンツ配送を要求してきたユーザが誰であるのかを正確に識別して、確実に課金することができなければならない。即ち、課金を行うために必要なデータ（例えば、クレジットカード番号、銀行口座番号、等）を登録していない第三者がこれらデータを登録しているユーザになりすましてコンテンツの配送を受けてしまうことを、防止しなければならない。そのため、登録されているIDコードとコンテンツ配送を行ったユーザのIDコードとを照合する認証システムが提案されている。

【0007】しかしながら、このようなIDコードによる認証システムでは、IDコードが第三者によって盗まれた場合においてこの第三者による盗用を防止する手ではない。なお、IDコードにパスワードを付する方式も提案されているが、盗まれた場合に第三者の盗用が可能であることには変わりがない。

【0008】そこで、本発明の第1の課題は、ユーザ（クライアント）とサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方において動的に作成することにより、第三者の盗用が不可能となるクライアント認証システムを提供することである。

【0009】また、単純なIDコードによって認証を行うシステムであるならば、ユーザがこのIDコードをマニュアルで入力できるので、コンテンツの配送要求を行った個人毎の認証も可能であるが、複雑な識別情報を扱う場合であると、識別情報の動的な作成は勿論、マニュアルによる識別情報の入力ですえも不可能となってしまう。従って、従来提案されていた認証システムでは、コンテンツの再生を行う再生装置が自動的に認証作業を実行し、この再生装置毎に認証を行うようになっていた。

【0010】しかしながら、再生装置毎に認証を行うのであると、複数の再生装置を有している場合には、再生装置毎に課金のためのデータを登録しなければならない。また、自己の課金のためのデータがサービス提供者に登録されている場合であっても、例えば他人に借りた再生装置でコンテンツを再生することは一切できなくなってしまう。このように硬直したシステムであると、上述した理由によりシステム普及はおぼつかない。

【0011】そこで、本発明の第2の課題は、ユーザが容易に携帯できるとともに複数の再生装置に対して共通に装着できるモジュールに、認証を行うためのデータ及び機能を持たせたクライアント認証システムを提供することである。

【0012】

【課題を解決するための手段】

(第1の課題を解決するための手段) 本発明によるクライアント認証システムの第1の態様は、上記第1の課題を解決するために、データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して配送されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証システムにおいて、前記データ供給装置は、前記クライアントに対応する第1の鍵を出力する鍵出力部と、前記クライアントからのアクセス要求に応じて乱数を発生する乱数発生手段と、前記鍵出力部において出力された第1の鍵によって前記乱数を暗号化することによって第1の認証子を出力する第1の暗号化手段と、前記クライアントに前記乱数を送信する第1の送信手段と、前記クライアントから第2の認証子を受信する第1の受信手段と、前記第1の認証子と前記第2の認証子とを比較して両者が一致している場合に当該クライアントからのアクセス要求であると認証する比較手段とを備え、前記クライアントは、前記データ供給装置にアクセス要求を行うアクセス要求手段と、前記データ供給装置から送信された前記乱数を受信する第2の受信手段と、前記第1の鍵と同一の第2の鍵を保持する鍵保持手段と、前記第2の鍵によって前記乱数を暗号化することによって前記第2の認証子を出力する第2の暗号化手段と、前記データ供給装置に前記第2の認証子を送信する第2の送信手段とを備えることを特徴とする(請求項1に対応)。

【0013】前記アクセス要求手段は、前記アクセス要求に際してそのクライアントに設定された固有の識別情報を前記データ供給装置に通知するとともに、前記鍵出力部は、各クライアントに固有の前記識別情報を加工することにより前記第1の鍵を生成するようにしても良い(請求項2に対応)。

【0014】前記データ供給装置は前記比較手段によって前記両認証子が一致すると判断された場合のみ前記データを前記クライアントに配送するようにしても良い(請求項3に対応)。

【0015】前記データ供給装置は暗号化された前記データを前記クライアントに配送するとともに、前記クライアントは前記暗号化された前記データを復号化する第1の復号化手段を備えるようにしても良い(請求項4に対応)。

【0016】前記データ供給装置は前記データを復号化するための第3の鍵を前記第1の鍵によって暗号化する第3の暗号化手段を備えているとともに、前記クライアントは前記暗号化された前記第3の鍵を前記第2の鍵によって復号化する第2の復号化手段を備え、前記第1の復号化手段はこの第2の復号化手段によって復号化された前記第3の鍵によって前記暗号化されたデータを復元するようにしても良い(請求項5に対応)。

【0017】前記データ供給装置は、前記暗号化されたデータを格納するための複数の格納装置を備えるとも

に、一方の格納装置に格納されている前記暗号化されたデータを前記第3の鍵を用いて復号化する第3の復号化手段と、第3の鍵を更新する鍵更新手段と、第3の復号化手段によって復号化されたデータを前記鍵更新手段によって更新された前記第3の鍵によって暗号化する第3の暗号化手段と、第3の暗号化手段によって暗号化されたデータを他の前記格納装置に格納する書込手段とを更に備えるように構成しても良い(請求項6に対応)。このように格納装置を二重化する事によりデータのバックアップができるとともに、暗号化した鍵をその都度更新するので、データのセキュリティを向上させることができる。

【0018】なお、前記第3の復号化手段、前記鍵更新手段、前記第3の暗号化手段、及び前記書込手段を一定時間毎に起動するようにしても良い(請求項7に対応)。本発明によるクライアント認証方法は、上記第1の課題を解決するため、データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して送出されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証方法において、前記クライアントは自己を識別する識別情報を付して前記データ供給装置にアクセス要求を行い、前記データ供給装置は、このアクセス要求に応じて乱数を発生してこの乱数を前記クライアントに送出するとともに、前記識別情報に対応する第1の鍵によって前記乱数を暗号化して第1の認証子に変換し、前記クライアントは前記第1の鍵と同一内容を有するものとして予め保持している第2の鍵によって前記乱数を暗号化して第2の認証子に変換するとともに、この第2の認証子を前記データ供給装置に送出し、前記データ供給装置は前記第1の認証子と前記第2の認証子とを比較して両者が一致した場合に前記クライアントからのアクセス要求があったことを認証することを特徴とする(請求項9に対応)。

(第2の課題を解決するための手段) 本発明の前記クライアント認証システムの第2の態様は、前記第1の態様におけるクライアントを、前記データを受信する本体部とこの本体部に対して着脱自在に設けられたモジュール部とから構成するとともに、少なくとも前記鍵保持手段及び前記第2の暗号化手段は前記モジュール部に備えるように構成したことを特徴とする(請求項8に対応)。なお、上述の識別情報を使用する場合には、この識別情報はこのモジュール部に格納しておく。また、上述の第1の復号化手段及び第2の復号化手段を設ける場合には、これら復号化手段をこのモジュール部に格納する。

【0019】

【作用】本発明の第1の態様によると、クライアントのアクセス要求手段がデータ供給装置にアクセス要求を行うと、このアクセス要求に応じて、データ供給装置の乱数発生部が乱数を発生するとともに、鍵出力部がこのクライアントに対応する第1の鍵を出力する。そして、第

1の通信手段は、アクセス要求元のクライアントに乱数を送信する。また、第1の暗号化手段は、鍵出力部において出力された第1の鍵によって乱数を暗号化することにより、第1の認証子を出力する。一方、クライアントの第2の受信手段が乱数を受信すると、第2の暗号化手段は、鍵保持手段が保持している前記第1の鍵と同一の第2の鍵によってこの乱数を暗号化することにより、第2の認証子を出力する。この第2の認証子は、第2の送信手段によってデータ供給装置に送信される。データ供給装置の第1の受信手段がこの第2の認証子を受信すると、比較手段が第1の認証子と第2の認証子とを比較して、両者が一致している場合に当該クライアントからのアクセス要求であると認証する。従って、通信インタフェース上で送信される識別のための情報(認証子)は暗号化されたものであって、その暗号化された結果は乱数に従って変化するので一定にはならない。そのため、第三者による盗用が不可能になる。

【0020】本発明の第2の態様によると、クライアントを構成する各構成部のうち、認証に必要なデータを保持する構成部(鍵保持手段)や認証に必要な処理を行うための構成部(第2の暗号化手段)のみを、本体部から着脱自在に設けたモジュール部に備えるようにしたので、誰の所有による本体部であっても、ユーザが自分のモジュール部を接続してデータの配送を受けることができる。

【0021】

【実施例】以下、図面に基づいて、本発明の一実施例の説明を行う。本実施例は、本発明によるクライアント認証システムを、デジタル・オーディオ・インタラクティブ・システムに適用したものである。なお以下の説明においては、コンテンツを再生するためのコンテンツ再生装置のことを、「サービスクライアント」という。

《実施例の構成》

(システムの全体構成) 本実施例によるデジタル・オーディオ・インタラクティブ・システムを図1に示す。このシステムは、多数のコンテンツを格納するとともにこのコンテンツを配送するためのサービス提供者側システム1と、コンテンツを再生するための多数の端末とから、構成されている。この端末には、パーソナルコンピュータ2、サービスクライアント6a、6b、及びDVDプレーヤ8が含まれている。また、パーソナルコンピュータ2にはリムーバブルディスク装置3が接続されている。また、第1のサービスクライアント6aには、SCSIインタフェースを介して光磁気ディスクドライブ4が接続されている。DVDプレーヤ8を除く各端末は、上位サービスレイヤインタフェースS1、及びアプリケーションサービスレイヤインタフェースS2を介して、サービス提供者側システム1に接続されている。

【0022】これら上位サービスレイヤインタフェースS1、及びアプリケーションサービスレイヤインタフェ

ースS2は、図2に示すDAVIC 1.0システムリファレンスモデルによって定義されたインタフェースである。この上位サービスレイヤインタフェースS1は、コンテンツを配送するためのインタフェースであり、具体的には、ケーブルテレビジョンシステムのケーブル、衛星回線、ISDN等である。また、アプリケーションサービスレイヤインタフェースS2は、アクセス制御情報を交換するためのインタフェースであり、ケーブルテレビジョンシステムのケーブル、ISDNを上位サービスレイヤインタフェースS1と兼用することができる他、アナログ電話網を用いることができる。

【0023】なお、図1に示した(S1)は、物理的運搬を意味する。即ち、サービス提供者から購入したコンテンツ入りのフロッピーディスクを運搬して、パーソナルコンピュータ1のリムーバブルディスク装置3にロードしたり、サービス提供者から購入したコンテンツ入りのビデオディスクを運搬して、DVDプレーヤ8にロードすることを意味する。このような物理的運搬も、S1のインタフェースに該当する。同様に、制御情報をFAX、メール等によって送信することも、S2のインタフェースに該当する。

【0024】本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、コンテンツ提供者又はサービス提供者から提供される有料のコンテンツまたは機密情報を第三者から容易に傍受されることを防ぐ目的のために、サービス提供者側システム1とサービスクライアント6との間に、セキュリティ機構を設けた。このセキュリティ機構は、サービス提供者側システム1から供給されるコンテンツが第三者によって悪用されたり転用されることを防止するために、このコンテンツを暗号化してサービスクライアント6に提供する。即ち、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、図2に示したDAVIC 1.0システムリファレンスモデルに基づき、セキュリティ・アンド・アクセス・コントロール機能を、サービス提供者側システム1及びサービスクライアント6に置いたものである。

【0025】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、サービスクライアント6に復号化機能を持たせるために、模倣や改造が難しいハードウェア機構を一部採用し、認証及び秘匿を実現した。

【0026】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、ユーザへの利便性を考慮し、復号化機能を実現するアルゴリズム、鍵管理、認証、秘匿、および課金に関する情報などユーザのセキュリティに付随する機能を、利用者が携帯可能なモジュール(以後、「MASC: Media Access and Security Card」と呼ぶ)5に収め、このMASC5をサービスクライアント6に脱着可能とした。そのた

め、このMAS C 5を何れかのサービスクライアント6に装着することにより、別個のサービスクライアント6であっても同様のサービスを受けることが可能となる。

【0027】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、他の標準化作業を尊重するため、サービスクライアント6側の認証方式は、ISO/IEC9798-2 に準拠した。また、鍵管理方式は、B-MACスクランブル放送で採用されている方式に準拠した。また、暗号登録方式は、ISO/IEC 9979に準拠し、鍵サイズおよび入出力データサイズのみ規定するとともに処理アルゴリズムは規定しないものとした。また、MAS C 5のサービスクライアント6との物理インタフェースは、DVB 方式案の一部を変更して採用した。

【0028】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、コンテンツ提供形態の多様化（ケーブル、衛星システム、パッケージ等）に対応できるように、拡張性の高いデータ構造、処理方式を採用した。

【0029】＜サービス提供者側システムの構成＞次に、図3を参照して、データ供給装置としてのサービス提供者側システム1の内部構成を説明する。図3に示すように、サービス提供者側システム1は、サーバ10と、このサーバ10と各々バス接続されたユーザプロフィール11、第1データファイル12、第2データファイル13、デジタル署名部14、認証部15、鍵更新処理部16、鍵管理部18、及び乱数発生器20と、サーバ10に夫々接続された衛星回線S、ケーブルテレビジョンシステムのケーブルC、及び電話網Nと、鍵更新処理部16に接続された鍵更新タイマ17と、鍵管理部18に接続されたサービスプロバイダID記憶部19とから、構成されている。

【0030】第1の送信手段及び第1の受信手段としてのサーバ10は、サービス提供者側システム1全体の制御を行うとともに、衛星回線S、ケーブルテレビジョンシステムのケーブルC、電話網Nを介してサービスクライアント6と通信を行う処理装置である。

【0031】ユーザプロフィール11は、各MAS CのIDが登録されているデータベースである。第1データファイル12は、暗号化された多数のコンテンツ及びこれらのID（タイトルID）を格納するデータベースである。第2データファイル13は、この第1データファイル12に格納されていたコンテンツを別の鍵を用いて再暗号化したもの及びそれらタイトルIDを格納するデータベースである。即ち、これらのデータファイル12、13に格納されるコンテンツは、一定時間毎に再暗号化されて、一方のデータファイルから他方のデータファイルに移されるのである。なお、これらデータファイル12、13に格納されるコンテンツには、予めMPEG-2規格により圧縮処理がなされている。

【0032】デジタル署名部14は、ユーザに対する課金額に対応した一定範囲のコンテンツ再生を許可するデータを、このデータが正しいことを論理的に証明するデジタル署名情報を付して、サービスクライアント6に送信する部分である。

【0033】認証部15は、当該サービス提供者側システム1に対して通信を行ってきたサービスクライアントに装着された個々のMAS C 5がユーザプロフィール11にそのIDが登録されているどのMAS C 5であるのかを調べる作業を行う。

【0034】乱数発生手段としての乱数発生器20は、この認証部15の作業において用いられる乱数を発生する。鍵出力部としての鍵管理部18は、認証部15におけるMAS Kの識別に用いる鍵（第1の鍵）を、ユーザプロフィール11に登録されているMAS CのIDから生成するとともに、各データファイル12、13に格納されている暗号化されたコンテンツを復元するための鍵（第3の鍵）を、対応するタイトルIDに基づいて生成する。

【0035】サービスプロバイダID記憶部19は、この鍵管理部18における鍵生成に用いられる当該サービス提供者側システムのID（サービスプロバイダID：IDP）を保持しているメモリである。

【0036】鍵更新処理部16は、一方のデータファイル12、13に格納されているコンテンツを鍵管理部18において生成されたタイトルIDに基づいて復元するとともに新たな鍵を作成し、復元されたコンテンツをこの新たな鍵によって暗号化して他方のデータファイル12、13に格納する。

【0037】鍵更新タイマ17は、この鍵更新処理部における処理のタイミングを規定するタイマである。

＜サービスクライアントシステムの構成＞次に、図4を参照して、サービスクライアントシステムの構成を説明する。

【0038】図4に示すように、サービスクライアントシステムは、衛星回線からの電波を受信するパラボラアンテナ22と、このパラボラアンテナ22に接続された衛星デコーダ23と、ケーブルテレビジョンシステムのケーブルに接続されたCATVアダプタ26と、光磁気ディスクドライブ4と、これら衛星デコーダ23、CATVアダプタ26、及び光磁気ディスクドライブ4に接続されたデータセクタ38と、このデータセクタ38に接続された本体部としてのサービスクライアント6と、このサービスクライアント6に装着されたモジュール部としてのMAS C 5と、電話網Nに接続されたモデム57とから、構成されている。

【0039】衛星デコーダ23は、パラボラアンテナ22によって受信された信号を復調する復調回路24と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ25とから、構成されている。デコーダ

25の出力端子は、データセクタ38の第1コネクタに接続される。

【0040】CATVアダプタ23は、ケーブルから受信された信号を復調する復調回路27と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ28とから、構成されている。デコーダ28の出力端子は、データセクタ38の第2コネクタに接続される。

【0041】光磁気ディスクドライブ4は、データセクタ38の第4コネクタに接続されたエンコーダ35と、このエンコーダ35によってエラー訂正及びビットの並び替えがなされたデータを変調する変調回路34と、光磁気ディスク30に対してデータの書込/読み出しを行うピックアップ31と、ピックアップ31によって読み出されたデータを復調する復調回路32と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ33と、光磁気ディスク30を回転させるとともにピックアップ31をトラッキングさせるドライブ回路36とから、構成されている。デコーダ33の出力端子は、データセクタ38の第3コネクタに接続される。

【0042】データセクタ38は、第1乃至第3コネクタから入力したデータを第4コネクタ又は第5コネクタに出力する。そのために、データセクタ38は、第1乃至第3の何れかのコネクタに接続線を接続するかを選択するスイッチSW1と、第4又は第5の何れかのコネクタに接続線を接続するかを選択するスイッチSW2とを備えている。

【0043】サービスクライアント6は、データセクタの第5コネクタに接続されたDL40、ホストCPU41、及びスイッチ42と、スイッチ42に接続されたデマルチプレクサ43と、このデマルチプレクサ43に接続された画像用MPEG伸長回路44と、この画像用MPEG伸長回路44に接続されたD/A変換器47と、デマルチプレクサ43に接続された音声用MPEG伸長回路45と、この音声用MPEG伸長回路45に接続されたD/A変換器48と、両MPEG伸長回路44、45に接続された同期回路46と、ホストCPU41に接続されたセクタベイロード対向テーブル49と、モデム57に接続されたインタフェース50とから、構成されている。

【0044】DL40は、ディレイライン装置であり、トグルバッファ又はFIFOメモリから構成された帯域変換装置である。スイッチ42はCPU41からの指示に従い、データセクタ38からの信号線又はMASC5からの信号線をデマルチプレクサ43に接続する。また、スイッチ42は、CPU41からの指示に応じて、回路を開く。

【0045】ホストCPU41は、当該サービスクライアント6全体の制御を行う制御装置である。また、ホス

トCPU41は、データセクタ38から受信したコンテンツが予め暗号化されているかどうかを解析する。そして、暗号化がなされていないのであればデータセクタ38からの信号線をデマルチプレクサ43に接続させる指示をスイッチ42に対して行い、暗号化がなされているのであればMASC5からの信号線をデマルチプレクサ43に接続させる指示をスイッチ42に対して行うとともに、MASC5に対して復号化を指示する。なお、ホストCPU41は、MASC5の制御CPU51からの指示があった場合には、コンテンツが暗号化されている場合であっても、スイッチ42に対してデータセクタからの信号線をデマルチプレクサ43に接続させる指示を行う。また、ホストSPU41は、データセクタ38からコンテンツを構成する各フレームを受信する毎に、MASC5に対して通知を行う。

【0046】デマルチプレクサ43は、コンテンツ中の音声データフレーム及び画像データフレームを分離する。そして、画像データフレームを画像用MPEG伸長回路(MPEG-2)44に出力し、音声データフレームを音声用MPEG伸長回路(MPEG-2)45に出力する。

【0047】MPEG伸長回路(MPEG-2)44、45は、MPEG規格で圧縮されたままの状態では送信されて来た画像データフレーム、又は音声データフレームを伸長して、画像又は音声を出力可能なフォーマットに復元する回路である。これらMPEG伸長回路(MPEG-2)44、45においてデータフレームの伸長をする際には、同期回路46によって出力の同期がとられる。即ち、同期回路46から出力される同期信号に同期して、各MPEG伸長回路(MPEG-2)44、45は、伸長されたデータフレームを出力するのである。

【0048】画像用MPEG伸長回路(MPEG-2)44からの出力は、D/A変換器47によってアナログ信号に変換される。このアナログ信号は、当該サービスクライアント2に接続されている図示せぬTVモニタ装置に向けて出力される。また、音声用MPEG伸長回路(MPEG-2)45からの出力は、D/A変換器48によってアナログ信号に変換される。このアナログ信号は、当該サービスクライアントに接続されている図示せぬスピーカに向けて出力される。

【0049】セクタベイロード対向テーブル49は、光磁気ディスク30の各セクタとフレームとの関係に対応させているテーブルである。即ち、光磁気ディスクドライブ4からのコンテンツを読み出している場合において、ホストCPU41によって各フレームが読みとられる毎に、このセクタベイロード対向テーブル49によってセクタとの対応が調べられるのである。そして、現在のセクタから全てのフレームが読み出された時には、セクタコントローラ37に対して、ピックアップ31のトラッキングを行うべき旨が指示されるのである。



【0050】第2の受信手段及び第2の送信手段としてのインタフェース50は、モデム57と電話網N(S2)を介して、サービス提供者側システム1のサーバ10と通信を行い、制御情報の送受信を行う。

【0051】次に、DL40、ホストCPU51、スイッチ42、及びインタフェース56に接続されるMASC5の説明を行う。サービスクライアント6に提供される各種コンテンツは、衛星通信の様に入手が容易な通信媒体を介して配送されることがあるので、その再生に対する課金方法を如何にするかが問題となる。また、このような通信媒体を介して配送されるコンテンツは第三者による盗用を防止するために予め暗号化された状態で流通されるので、これを復号化する必要がある。そのため用いられるのがMASC5である。即ち、MASC5は、ホストCPU41からの指示に応じて、DL40を介して受信したコンテンツを復号化してスイッチ42に送信する。また、MASC5は、ホストCPU41がフレーム41を受信する毎に行う通知をカウントして、課金カウンタ値Xを減算する。この課金カウンタ値Xとは、ユーザがサービス提供者側システムのデジタル署名部14に対して代金支払いを了承することによって当該SD回路に書き込まれたポイントである。MASC5は、この課金カウンタ値Xが0になった時に、ホストCPU41に対して、スイッチ42を開かせるのである。

【0052】なお、このMASC5は、サービスクライアント6のカードスロット（たとえばPCMCIA準拠のカードスロット）内に着脱自在に装着されたICカードの形態で実現される。このようなICカードの形態にしておけば、SD回路の運搬が容易となる。

【0053】このMASC5は、相互にバス接続された制御CPU51、DES(Data Encryption Standard)53、課金情報記憶部55、ROM57、並びにI/O装置52、54、及び56から構成されている。

【0054】制御CPU51は、サービスクライアント6内のホスト制御CPU14に接続されており、ホストCPU41からの指示に応じてDES53に対して復号化処理を実行させる。また、制御CPU51は、ホストCPU41からのフレーム受信通知に応じて課金部55内に格納されている課金カウンタ値Xを減算するとともに、この課金カウンタ値Xが0になったときは、CPU41に対して、スイッチ42を開かせる。また、制御CPU51は、I/O装置56、インタフェース50及びモデム57を介してサービス提供者側システム1との間で通信を行って、アクセス要求、デジタル署名、及びユーザ認証のために必要な処理を行う（アクセス要求手段に対応）。

【0055】鍵保持手段としてのROM56は、この制御CPU51における処理に必要な諸データ（例えば、当該MASC5を識別するための識別ID<sub>i</sub>、固有の識

別情報）、当該MASC5に固有のものとして備えられた個別鍵K<sub>i</sub>、[第2の鍵]）を記憶しているメモリである。

【0056】課金情報記憶部55は、上述した課金カウンタ値Xを格納しているメモリである。なお、課金情報記憶部55内において、課金カウンタ値Xは暗号化されている。従って、ユーザがこの課金情報記憶部55を解析して課金カウンタ値Xを書き換えることは、不可能である。

【0057】第2の暗号化手段、並びに第1及び第2の複合化手段としてのDES7は、I/O装置52を介してDL40から受け取ったコンテンツを復号化する機能、及び制御CPU51が行うデジタル署名及びユーザ認証に際して必要な暗号化及び復号化を行う機能を有する。DES7により復号化されたコンテンツ（画像フレーム、音声フレーム）は、I/O装置54を通じて、スイッチ42に送出される。

《実施例における処理内容》次に、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいて、サービス提供者側システム1とサービスクライアント6との間で実行される制御処理を、フローチャート及びこのフローチャートの各ステップにおいて実現される機能を示すための機能ブロック図を参照して、説明する。

【0058】サービスクライアント6がサービス提供者側システム1管理の情報にアクセスする場合、安全な通信制御手段が必要となる。これはサービスクライアント6とサービス提供者側システムとの間を結ぶS1とS2の形態により異なる。

【0059】（コンテンツ情報送信制御処理）先ず最初に、サービスクライアント6側からサービス提供側システム1に対して何れかのコンテンツの配送を要求する際の制御処理について説明する。この場合、S1、S2のインタフェースが秘密保持性が高い通信媒体であるか否かによって、制御を異にする。なぜならば、秘密保持性が低い通信媒体によってコンテンツを配送する場合には、第三者による盗用やデータ改ざんを防ぐために暗号化する処理が不可欠だからである。

【0060】＜秘密保持性が高い通信媒体によるコンテンツ情報供給制御＞図5は、S1、S2の形態を、例えば光ファイバケーブル（ケーブルテレビジョンシステムのケーブル、等）のように、データ盗聴やデータ改ざんが比較的困難な信頼できるネットワークとした場合における制御内容を示す。この場合、サービスクライアント6側の不正アクセスのみが問題となる。従って、アクセス権確立のための認証が重要となる。

【0061】この場合の運用手順の概略を説明すると、最初にユーザは、サービスクライアント6にMASC5を挿入する。すると、サービスクライアント6は、MASC5の識別ID(ID<sub>i</sub>)を読み取り、その識別ID

(ID<sub>i</sub>)をサービス提供者側システムへ通知する。すると、サービス提供者側システム1は、何れのMAS C5であるかを認証する。次に、サービス提供者側システム1は、要求されたコンテンツをサービスクライアント6に向けて配送し、課金システムを動作させる。その結果、サービスクライアント6は、コンテンツを入手する。

【0062】[アクセス要求]図5における最初のステップ01では、サービスクライアント6は、サービス提供者側システム1に対してアクセス要求を行う。この前提として、サービスクライアント6が所有するMAS C5には、モジュール固有の識別ID(ID<sub>i</sub>)、個別鍵K<sub>i</sub>、及び認証アルゴリズムEK(X)が安全に格納されている。

【0063】ユーザは、このMAS C5を任意のサービスクライアント6へ接続し、図示せぬ操作キーを介してサービス提供者側システムの識別ID(サービスプロバイダID:ID<sub>p</sub>)を入力する。すると、図6(1)に示すように、サービスクライアント6は、サービス提供者側システムへのデータファイルアクセス要求コマンド、及びモジュール固有の識別IDに、サービス提供者側システムのデスティネーション[サービス提供者側システムの識別ID(ID<sub>p</sub>)とサービスクライアント6の識別ID(アドレス)とを結合したもの]を付して、S2インタフェースを介してサービス提供者側システム1に送信する。なお、この時、サービスクライアント5は、配送を求めるコンテンツのタイトルID(ID<sub>T</sub>)を、サービス提供者側システム1に送信する。

【0064】[認証処理]図5における次のステップ02では、サービス提供者側システム1によるサービスクライアントの認証処理を行う。このサービスクライアント認証は、当事者以外の第三者によるサービス提供者側システム1のデータファイルへの不正アクセス阻止を目的に実行される。ここでは、ISO/IEC 9798-2を利用し、当事者間で互いに共有する秘密の鍵データが同一であることにより認証を行う。

【0065】サービス提供者側システム1がアクセス要求をしたサービスクライアント6の正当性を認証する場合には、図6に示すような手順で認証処理を行う。尚、この認証のための通信は、S2インタフェースを介して行われる。

【0066】サービス提供者側システム1のサーバ10がサービスクライアント6からのアクセス要求を受信すると(1)、鍵管理部18内の第1鍵生成部(鍵出力部)182は、受信したMAS C識別ID(ID<sub>i</sub>)がユーザプロフィール11に登録されていることを確認し、ユーザプロフィール11内の当該識別ID(ID<sub>i</sub>)を基に、プロバイダ管理の第1マスタ鍵81を使ってクライアント個別鍵(第1の鍵)K<sub>i</sub>を生成する。この第1マスタ鍵81は、MAS C5内に格納されてい

る個別鍵(第2の鍵)K<sub>j</sub>が生成された際に用いられたマスタ鍵と同一である。従って、受信したMAS C識別ID(ID<sub>i</sub>)とユーザプロフィール11内に登録されている識別ID(ID<sub>i</sub>)とが同一である限り、MAS C5内の個別鍵K<sub>i</sub>と全く同じクライアント個別鍵K<sub>i</sub>が生成されることになる。

【0067】これと同時に、サービス提供者側システム1内の乱数発生部20は、乱数Rを発生する。この乱数Rは、認証部15に入力されるとともに、サーバ10にも入力される。サーバ10は、この乱数Rにサービスクライアント向けデスティネーション[サービスクライアント6の識別ID(アドレス)とサービス提供者側システムの識別ID(ID<sub>p</sub>)とを結合したもの]を付けて、サービスクライアント6へ送信する(2)。

【0068】サービス提供者側システム1からの情報を受信したサービスクライアント6は、情報に含まれる乱数RをMAS C5に与える。すると、MAS C5は、MAS C識別ID(ID<sub>i</sub>)に乱数Rを結合して、これを個別鍵K<sub>i</sub>によって暗号化することにより、第2の認証子を生成する。サービスクライアント6は、この第2の認証子にサービス提供者側システムのデスティネーションを付して再びサービス提供者側システム1へ送り返す(3)。

【0069】このクライアント情報を受信したサービス提供者側システム1は、この情報に含まれる第2の認証子を、認証部15内の比較器(比較手段)152へ設定する。更に、認証部15内の第1暗号化部(第1の暗号化手段)151は、サービスクライアント5から受信したMAS C識別IDと乱数発生部20から受信した乱数Rとを結合して、これを鍵生成部182にて生成されたクライアント個別鍵K<sub>i</sub>によって暗号化することにより、第1の認証子を生成する。第1暗号化部151は、この第1の認証子を比較器152へ設定して、先に設定した第2の認証子と比較させる。比較器152において両認証子が一致すれば、サービスクライアント5及びサービス提供者側システム1間に同一の個別鍵K<sub>i</sub>が保有されていることになるので、認証部15は、当該サービスクライアントを通信当事者として認証し、後の処理を可能とする。これに対して、両認証子が相違している場合には、そのMAS C5に対応する課金用データが登録されていないサービスクライアントであると判断して、後の処理を禁止する。このように、本実施例による認証方式によると、認証の対象となる個別鍵K<sub>i</sub>自体がインタフェース上を送信されるのではなく、アクセス要求の都度生成される乱数をこの個別鍵K<sub>i</sub>で暗号化した認証子が送信されるだけである。従って、第三者が乱数Rを盗んだとしても、個別鍵K<sub>i</sub>の内容を知らない限り、認証子を生成することは不可能である。また、認証子自体を盗んだとしても、既に正規のユーザに対する認証が済んでいる場合には、この認証子に対する乱数Rは認証

部15にセットされていないので、当該認証子は既に無効となっている。このように何れにしても第三者の不正なアクセスは、阻止されるのである。

【0070】なお、サービスクライアント6がサービス提供者側システム1を認証するときには、上記のサービスクライアント6及びサービス提供者側システム1の立場を入れ換えて同様な手順を実行することにより、サービスクライアント6がサービス提供者側システム1を認証することが可能となる。

【0071】また、認証プロセスで用いるパラメータは、認証子の生成アルゴリズムにより異なる。例えば生成アルゴリズムにDES (DATA ENCRYPTION STANDARD) を採用した場合、以下の通りである。

【0072】

乱数R : 32 ビット

MASC識別ID: 32 ビット( ECB入力時には残り32ビットはパディングする)

個別鍵K<sub>i</sub> : 56 ビット

マスタ鍵KM : 168ビット(56 ビット×3)

サービス提供者側システム1の利用モード: TRIPPLE ECB(ELECTRONIC CODE BOOK)(個別鍵生成、乱数生成)

サービスクライアントの利用モード: ECB(認証処理)

【コンテンツ情報配送処理】図5における次のステップ03では、サービスクライアント6からのコンテンツ情報配送処理を行う。即ち、サービス提供者側システム1は、サービスクライアント5から要求されたタイトルID(ID<sub>T</sub>)に対応するコンテンツ(暗号化コンテンツ)を、何れかのデータファイル12、13から読み出して復号化する。そして、S1インタフェースを介して、復号化されたコンテンツをサービスクライアント6に送信するのである。

【0073】コンテンツを受け取ったサービスクライアント6は、これを一旦光ディスクドライブ4に送信して光ディスク30に書き込むか、そのままCPU42に流す。ホストCPU42はこのコンテンツが暗号化されていないものであると解析して、スイッチ43をデータセレクタ側に切り換える。従って、コンテンツはそのままデマルチプレクサ43にて画像フレームと音声フレームに分離されて、夫々MPEG伸長回路44、45にて伸長され、DA変換器47、48にてアナログ信号に変換される。そして、画像信号は図示せぬTVモニターへ送信され、音声信号は図示せぬスピーカへ送信される。

【0074】また、ホストCPU41は、コンテンツを構成する各フレームを読み込む毎に、MASC5内の制御CPU51に通知を行う。この制御CPU51は、通知の数をカウントして、課金情報記憶部55内の課金カウント値Xを減算する。そして、この課金カウント値Xが0になると、制御CPU51は、ホストCPU41に対して、スイッチを42を開かせる。従って、課金額に対応する使用許可量を越えたコンテンツの使用が阻止さ

れるのである。

【0075】＜一般のネットワークによるコンテンツ情報供給制御＞図7は、S1、S2の形態を、無線路や様々な迂回路を経由する一般のネットワーク形態とした場合における制御内容を示す。この形態では、データ盗聴やデータ改ざん行為が十分起こり得るので、上述のサービスクライアント認証処理の他、データ暗号化を如何に行うかが重要である。

【0076】この場合の運用手順の概略を説明すると、最初に利用者は、サービスクライアント6にMASC5を挿入する。すると、サービスクライアント6は、MASC5の識別ID(ID<sub>i</sub>)を読み取り、その識別ID(ID<sub>i</sub>)をサービス提供者側システム1へ通知する。すると、サービス提供者側システム1は、何れのMASC5であるかを認証する。次に、サービス提供者側システム1は、サービスに必要な鍵(KG<sub>i</sub>)をサービスクライアント6に配送する。このようにして、サービスクライアント6は、必要な鍵(KG<sub>i</sub>)を入手する。その後、サービス提供者側システム1は、要求されたコンテンツをサービスクライアント6に向けて配送し、課金システムを動作させる。その結果、サービスクライアント6は、この鍵(KG<sub>i</sub>)を利用してコンテンツを入手する。

【0077】[アクセス要求] 図7における最初のステップ11では、サービスクライアント6は、図8に示すように、サービス提供者側システム1に対してアクセス要求を行う。このアクセス要求の内容は、図5におけるステップ01と同じなので、その説明を省略する。

【0078】[認証処理] 図7における次のステップ12では、サービス提供者側システム1は、図8に示すように、サービスクライアント6の認証を行う。この認証処理は、図5におけるステップ12と同じなので、その説明を省略する。

【0079】[鍵配送処理] 図7における次のステップ13では、サービス提供者側システム1は、図8に示すように、暗号化コンテンツの復元用の鍵(KG<sub>i</sub>)の配送を行う。この鍵配送は、暗号化されている各種コンテンツの情報をサービスクライアント6側で円滑に復号させる為に、S2インタフェースを使って行われる。

【0080】即ち、サービス提供者側システム1は、サービスクライアント6に装着されたMASC5が発信してきたMASC識別ID(ID<sub>i</sub>)から、クライアント個別鍵K<sub>i</sub>を生成しする(このクライアント個別鍵K<sub>i</sub>としてクライアント認証において用いたものを流用しても良い)。サービス提供者側システム1は、クライアント個別鍵K<sub>i</sub>鍵によってサービスプロバイダID(ID<sub>P</sub>)及びタイトル鍵KG<sub>1</sub>を暗号化し、サービスクライアント向けデスティネーション[サービスクライアント6の識別ID(アドレス)とサービス提供者側システム1の識別ID(アドレス)とを結合したもの]を付して、

MASC5に送信する。サービス提供者側システム1からの暗号化鍵情報は、MASC5において復号化され、タイトル鍵KG<sub>1</sub>が得られる。以後、S1インタフェースで送られてくる暗号化コンテンツが、このタイトル鍵KG<sub>1</sub>によって復号化される。

【0081】この鍵配送処理の内容を、図9の機能ブロック及び図10のサブルーチンフローチャートに基づいて説明する。なお、説明の都合上、現時点において第1データファイル12に暗号化コンテンツが格納されているとし、これを「旧データファイル」と称するものとする。

【0082】図10において、最初のステップ21では、サービス提供者側システム1の鍵管理部18内に備えられたスイッチSW4を、旧データファイル12側に切り換える。そして、サービスクライアント5から要求されているタイトルに対応するタイトルID(IDT)を、スイッチSW4を介して旧データファイル12から読み出す。第2鍵生成部184は、読み出したタイトルID(IDT<sub>1</sub>)を第2マスタ鍵185に基づいて暗号化し、タイトル鍵(第3の鍵)KG<sub>1</sub>を生成する。

【0083】次のステップ22では、鍵管理部18内の第2暗号化部(第3の暗号化手段)183は、サービスプロバイダID記憶部19から受信したサービスプロバイダID(IDP)と、第2鍵生成部184から受信したタイトル鍵KG<sub>1</sub>とを、結合する。そして、第2暗号化部183は、認証処理時において第1鍵生成部182が生成したクライアント個別鍵K<sub>1</sub>に基づいて、これらサービスプロバイダID(IDP)及びタイトル鍵KG<sub>1</sub>を暗号化し、サーバ10に転送する。サーバ10は、受け取ったサービスプロバイダID及びタイトル鍵KG<sub>1</sub>の暗号化情報を、S2インタフェースを介してサービスクライアント6に配送する。

【0084】次のステップ23では、サービスクライアント6は、サービスプロバイダID及びタイトル鍵KG<sub>1</sub>の暗号化情報をMASC5に配送する。MASC5内の第1復号化部(第2の複合化部)101(DES53)は、MASC6のROM57に内蔵されている個別鍵K<sub>1</sub>を用いてこの暗号化情報を復号化し、サービスプロバイダID及びタイトル鍵KG<sub>1</sub>を獲得する。そして、このサービスプロバイダID(IDP)を比較器102にセットする。

【0085】次のステップ24では、MASC6内の比較器102は、第1復号化部101によってセットされたサービスプロバイダID(IDP)とアクセス要求時に図示せぬ操作キーを介して入力されたサービスプロバイダID(IDP)103とを、比較する。そして、両者が一致している場合には、処理をステップ25に進め、不一致の場合には、処理をステップ27に進める。

【0086】ステップ27において、受信不可能である旨がサービスクライアント5側に通知され、S2イン

タフェースを介してサービス提供者側システム1のサーバ10に転送される。

【0087】次のステップ28では、サービス提供者側システム1のサーバ10は、第2暗号化部183から受け取ったサービスプロバイダID(IDP)及びタイトル鍵KG<sub>1</sub>の暗号化情報を、S2インタフェースを介して再度MASC5側へ配送する。その後、処理はステップS23に戻される。

【0088】これに対して、ステップ25では、MASC6内のスイッチSW3が閉じられ、第1復号化部101において復元されたタイトル鍵KG<sub>1</sub>が第2復号化部(第1の復号化手段)104(DES53)にセットされる。それとともに、受信可能である旨がサービスクライアント5側に通知され、S2インタフェースを介してサービス提供者側システム1のサーバ10に転送される。

【0089】ステップ26において、サービス提供者側システム1のサーバ10は、スイッチSW1を閉じて、データファイル12からタイトル鍵KG<sub>1</sub>に対応するタイトルの暗号化コンテンツを読み出す。

【0090】[コンテンツ情報配送処理]図7のステップ14において実行されるコンテンツ情報配送処理は、図10のステップ26の直後に実行される。

【0091】即ち、図11に示すように、サーバ10は、データファイル12から読み出した暗号化コンテンツを、S1インタフェースを介してサービスクライアント6に配送する。サービスクライアント6は、この暗号化コンテンツをMASC5に転送する。MASC5の第2復号化部104(DES53)は、セットされたタイトル鍵KG<sub>1</sub>を用いてこの暗号化コンテンツを復号化する。

【0092】図4を用いてこの復号化を具体的に説明する。コンテンツを受け取ったサービスクライアント6は、これを一旦光ディスクドライブ4に送信して光ディスク30に書き込むか、そのままCPU42に流す。ホストCPU42はこのコンテンツが暗号化されているものであると解析して、スイッチ43をMASC側に切り換えるとともに、MASC5の制御CPU51に対して、復号化処理を指示する。この指示に応じて、制御CPU51は、暗号化コンテンツをDL40及びI/O装置52を介して読み込み、DES53(第1復号化部101、第2復号化部104)によって復号化を行う。このDES53には、インタフェース50及びI/O装置56を介して受信したタイトル鍵KG<sub>1</sub>がセットされているので、このタイトル鍵KG<sub>1</sub>を用いて複合化する。複合化されたコンテンツは、I/O装置54を介してスイッチ42に送信される。

【0093】コンテンツは、スイッチ42からデマルチプレクサ43に転送され、このデマルチプレクサ43にて画像フレームと音声フレームに分離されて、夫々MP

EG伸長回路44、45にて伸長され、DA変換器47、48にてアナログ信号に変換される。そして、画像信号は図示せぬTVモニタへ送信され、音声信号は図示せぬスピーカへ送信される。

【0094】また、ホストCPU41は、コンテンツを構成する各フレームを読み込む毎に、MASC5内の制御CPU51に通知を行う。この制御CPU51は、通知の数をカウントして、課金情報記憶部55内の課金カウント値Xを減算する。そして、この課金カウント値Xが0になると、制御CPU51は、DES53による復号化を中止するとともに、ホストCPU41に対してスイッチを42を開かせる。従って、課金額に対応する使用許可量を越えたコンテンツの使用が阻止されるのである。

【0095】このように、本実施例のキー配送処理によれば、データファイル12に格納されている各コンテンツ毎に、別個の復元用鍵(タイトル鍵KG<sub>11</sub>)を生成した。従って、同一のユーザが同じキーを用いて他のタイトルのコンテンツを再生することが防止できる。また、このタイトル鍵KG<sub>11</sub>は、MASC5毎に用意された鍵(個別鍵K<sub>i</sub>)によって暗号化されるので、第三者が暗号化された鍵を傍受したとしても、タイトル鍵KG<sub>11</sub>を復元することは不可能である。従って、第三者の盗用が阻止できる。

【0096】(ローカル課金処理)次に、コンテンツ情報を再生するために必要な課金カウント値Xの加算を申込むためのローカル課金処理を、図12に基づいて説明する。この課金カウント値Xの加算値は、サービスクライアント6からサービス提供者側システム1に対して、代金の銀行口座からの引き落としを条件に申し込まれ、サービス提供者側システム1によってMASC5に書き込まれる。このように、本実施例では、課金カウント値Xの管理をMASC5において行っているため、特にデータ改ざん防止に重点が置かれる。よって、サービス供給者側システム1がこの加算値の正当性を証明するために加算値情報に付すデジタル署名が重要となる。従って、サービス提供者側システム1には、予め、MASC5毎に、暗証番号が登録されているものとする。

【0097】[アクセス要求]図12における最初のステップ31では、サービスクライアント6は、図13に示すように、サービス提供者側システム1に対してアクセス要求を行う。このとき、サービスクライアント6は、サービス提供者側システム1への課金カウント値増加要求コマンド、及びMASC固有の識別IDに、サービス提供者側システムのデスティネーション[サービス提供者側システムの識別ID(サービスプロバイダID:IDP)とサービスクライアント6の識別ID(アドレス)とを結合したもの]を付して、S2インタフェースを介してサービス提供者側システム1に送信する。

【0098】[認証処理]図12における次のステップ

32では、サービス提供者側システム1は、図13に示すように、サービスクライアント6の認証を行う。この認証処理は、図5におけるステップ02と同じなので、その説明を省略する。

【0099】[デジタル署名処理及び課金カウント値の書込処理]図12における次のステップ33では、サービスクライアント6においてデジタル署名が行われ、次のステップ34では、サービス提供者側システム1による課金カウント値Xの補充処理が行われる(図13参照)。

【0100】即ち、ユーザによるメッセージの認証は、サービス提供者側システム1とサービスクライアント5との間で、課金に関わるセンシティブデータをやりとりするときに、通信路上での第三者によるデータの改竄行為やサービスクライアント6でのユーザによるデータ改竄行為を阻止し、当事者間で円滑なトランザクション行為を達成するために、用いられる。ここでは、ISO 8731-1に基づくMAC(MESSAGE AUTHENTICATION CODE)方式を利用する。

【0101】サービス提供者側システム1のデジタル署名部14は、ユーザの銀行口座から引き落とす金額に対応する補充カウンタ値のデータブロック(DATA OF MENEY)140を、送信用フレームFに格納する。補充カウンタ値のデータブロック(DATA OF MENEY)140は、また、当該MASC5についての加算履歴回数に応じてインクリメントされる通番(IV)によって署名処理される(ステップ33)。即ち、排他OR回路142及び第3暗号化部143において、暗証番号(IV)を用いて、補充カウンタ値のデータブロック(DATA OF MENEY)140が暗号化されるのである。このような署名処理の最終処理結果(MAC)は、サービス提供者側システム1が補充カウンタ値の正当性を証明するためのデータとして、送信用フレームFに格納される。この送信用フレームFは、S2インタフェースを介して、サービスクライアント6に装着されたMASC5に送信される(ステップ34)。

【0102】MASC5は、受信した送信用フレームFに対して、サービス提供者側システム1側と同一処理を行う。即ち、送信用フレームFから補充カウンタ値のデータブロック(DATA OF MENEY)140を読み出す。そして、排他OR回路106及び暗号化回路106(DES53)において、補充履歴回数に応じてインクリメントされる通番(IV)を用いて、補充カウンタ値データブロックの全てに対して署名処理を行う。なお、この通番(IV)は、通常であれば、サービス提供者側システム1のデジタル署名部14に格納されている通番(IV)に同期している。次に、比較器107において、署名処理の結果生成されたMACの値(MAC')と送信用フレームFに格納されたMAC141の値とを比較する。比較の結果、両値が一致した時には、送信用フレー

ΔFに格納された補充カウンタ値のデータブロック (DATA OF MENEY) 140が正しい金額データであると判断し、スイッチSW6を閉じる。すると、この補充カウンタ値が、課金情報記憶部55に格納されている課金カウンタ値Xに加算される。

【0103】以上の結果、ユーザが送信用フレームFから補充カウンタ値を読み出してこれを書き換えた場合には、この書き換えた補充カウンタ値が課金カウンタ値Xに加算できなくなってしまうので、不正が防止できる。

【0104】このデジタル署名処理に用いられるパラメータは以下の通りである。

暗号化処理 : DES  
署名鍵 : 56ビット  
MAC : 32ビット(64ビット出力の左32ビットを抽出)  
金額データ : 64ビットブロック単位(不足分の32ビットはパディングビットを挿入)

(鍵の更新処理) 次に、一定時間毎に、旧データファイル12に格納されたコンテンツを新規なタイトル鍵KG<sub>1</sub>によって暗号化し直して新データファイル13に格納するための処理を図9のブロック図及び図14のフローチャートを参照して説明する。

【0105】即ち、サービス提供者側システム1で管理する各種タイトルのコンテンツは、それぞれのタイトル鍵KG<sub>1</sub>で予め暗号化されているが、同一の鍵で恒久的に暗号化した場合、解読の危険性が高まる。この為、タイトル鍵KG<sub>1</sub>の定期的更新を行って、暗号化をし直す必要があるのである。また、新たに追加されたタイトルのコンテンツに対しても、その都度タイトルに応じたタイトル鍵KG<sub>1</sub>で暗号化する必要がある。そのため、本実施例では、データファイル第1のデータファイル12及び第2のデータファイル13に分け、一方のデータファイルに現在稼働中の暗号化情報を格納するとともに(旧データファイル)、他方のデータファイルには図14の鍵の更新処理を実行することにより新たな暗号化コンテンツを格納するのである(新データファイル)。この図14の処理の前提として、鍵管理部18の第2マスタキー185と鍵更新処理部16の第2マスタ鍵163とは全く同じものであるとする。また、一度使用したタイトル鍵KG<sub>1</sub>は再使用を行うことなく使い捨てられるので、タイトル鍵KG<sub>1</sub>の生成に用いられる第2マスタ鍵163、185は、鍵更新の都度変更される。

【0106】図14の処理は鍵更新タイマ17に設定された周期毎にスタートする。即ち、本実施例では、タイトル鍵KG<sub>1</sub>の更新を、プログラムのサイクル及び安全係数を考慮に入れ、例えば一週間毎に行うようにしている。なお、図14の処理のスタートタイミング、即ち、新タイトル鍵KG<sub>1</sub>によって暗号化され直した新コンテンツの新データファイルへ格納するタイミングは、旧データファイル稼働中であることは、言うまでもない。ま

た、第1データファイル12を旧データファイルとする場合には、スイッチSW1を閉じ、スイッチSW2を開き、スイッチSW4を第1データファイル12側とし、スイッチSW5を第2データファイル側13とする。これに対して、第2データファイル13を旧データファイルとする場合には、これらと全く逆にする。

【0107】図14の処理において最初のステップ41では、鍵更新処理部16の復号処理部(第3の復号化手段)161に、第2鍵生成部184において現在のタイトルID(IDT<sub>1</sub>)に基づいて生成されたタイトル鍵KG<sub>1</sub>をセットする。

【0108】次のステップ42では、旧データファイル12に格納されている当該タイトル鍵KG<sub>1</sub>に対応する暗号化コンテンツを鍵更新処理部16の復号装置161にセットして、タイトル鍵KG<sub>1</sub>に基づいて復号を行う。

【0109】次のステップ43では、鍵更新処理部16の第3鍵生成部(鍵更新手段)164は、新データファイルに予め格納されている何れかのタイトルID(IDT<sub>1</sub>)を第2マスタ鍵163により暗号化して、新タイトル鍵KG<sub>1</sub>を生成する。第4暗号化部(第3の暗号化手段)162は、復号されたコンテンツを新タイトル鍵KG<sub>1</sub>に基づいて暗号化し直す。

【0110】次のステップ44では、第4暗号化部162が暗号化し直した暗号化コンテンツを、新データファイル13に書き込む(書込手段に対応)。次のステップ45では、鍵更新タイマ17によってある期限(例えば毎日曜日の深夜以降)まで待ち、各スイッチSW1、2、4、5を切り換える。例えば、第1データファイルを旧データファイルとしていた場合には、スイッチSW2を閉じ、スイッチSW1を開き、スイッチSW4を更新側に切り換え、スイッチSW5を旧データファイル12側に切り換える。これより、新データファイル13に格納されているタイトルID(IDT<sub>1</sub>)を鍵管理部18に送信可能となり、新データファイル13に格納されている暗号化コンテンツをサーバ10に送信可能となるとともに、この新データファイルを旧データファイルとして扱う次の更新処理が可能となる。このステップ44の処理が完了すると、処理が図10のステップ21に渡される。

【0111】(MASCの緊急対策) ユーザ側で万一MASC5の紛失又は盗難に遭遇した場合、サービス提供者は、緊急に鍵の破壊及びMASK5の再発行を行う。即ち、ユーザは、MASC5の紛失又は盗難の事実が確認されたなら、電話等の通信手段を使って直ちにサービス提供者にそのむね連絡する。このときユーザは、自身の名前、住所、連絡先をサービス提供者に通知する。次に、サービス提供者は、サービス提供者側システム1のプロファイルデータでユーザを確認後、ユーザに対して電話によるコールバックを行う。そして、サービス提供

者及びユーザ間で確認及び合意がとれれば、サービス提供者は、プロフィールから該当ユーザデータ全てを抹消し、対応するMASC5のID(ID<sub>i</sub>)を永久欠番とする。その後、ユーザは、サービス提供者又は近くの特約店或いは代理店へ行き、再登録の申請を行い、新しいID(ID<sub>i</sub>)付MASC5を発行してもらう。

【0112】

【発明の効果】以上のように構成された本発明のクライアント認証システムの第1の態様によると、ユーザ(クライアント)とサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方において動的に作成するので、第三者の盗用が不可能となる。

【0113】また、本発明のクライアント認証システムの第1の態様によると、ユーザが容易に携帯できるとともに複数の再生装置に対して共通に装着されるモジュールに、認証を行うためのデータ及び機能を持たせることができるので、再生装置が自己のものか否かに拘わらずコンテンツを再生できるとともに、サービス提供者は確実にコンテンツ再生代金を徴収することができる。

【図面の簡単な説明】

【図1】 本発明の一実施例によるクライアント認証システムが適用されたデジタル・オーディオ・インタラクティブ・システムの概略図

【図2】 図1のデジタル・オーディオ・インタラクティブ・システムに対応するシステムリファレンスモデルを示す図

【図3】 図1のサービス提供者側システムの構成を示すブロック図

【図4】 図1のサービスクライアント側システムの構成を示すブロック図

\*【図5】 秘密保持性が高い通信媒体によるコンテンツ情報供給制御を示すフローチャート

【図6】 認証処理に関連する構成を示すブロック図

【図7】 一般のネットワークによるコンテンツ情報供給制御を示すフローチャート

【図8】 鍵配送処理を示すタイムアロー図

【図9】 鍵配送処理に関連する構成を示すブロック図

【図10】 鍵配送処理の内容を示すフローチャート

【図11】 コンテンツ配送処理を示すタイムアロー図

【図12】 ローカル課金処理の内容を示すフローチャート

【図13】 デジタル署名処理に関連する構成を示すブロック図

【図14】 鍵の更新処理の内容を示すタイムアロー図

【符号の説明】

1 サービス提供者側システム

5 MASC

6 サービスクライアント

10 サーバ

11 ユーザプロフィール

12 第1データファイル

13 第2データファイル

14 デジタル署名部

15 認証部

16 鍵更新処理部

18 鍵管理部

20 乱数発生器

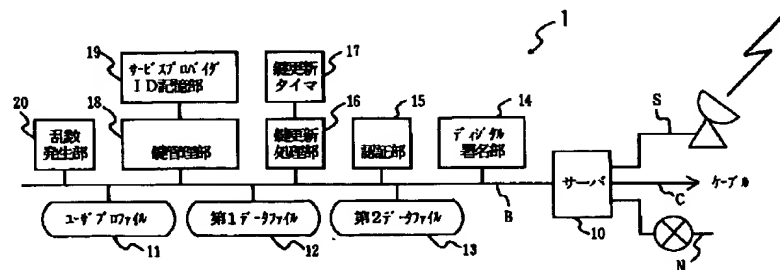
53 DES

55 課金情報記憶部

57 ROM

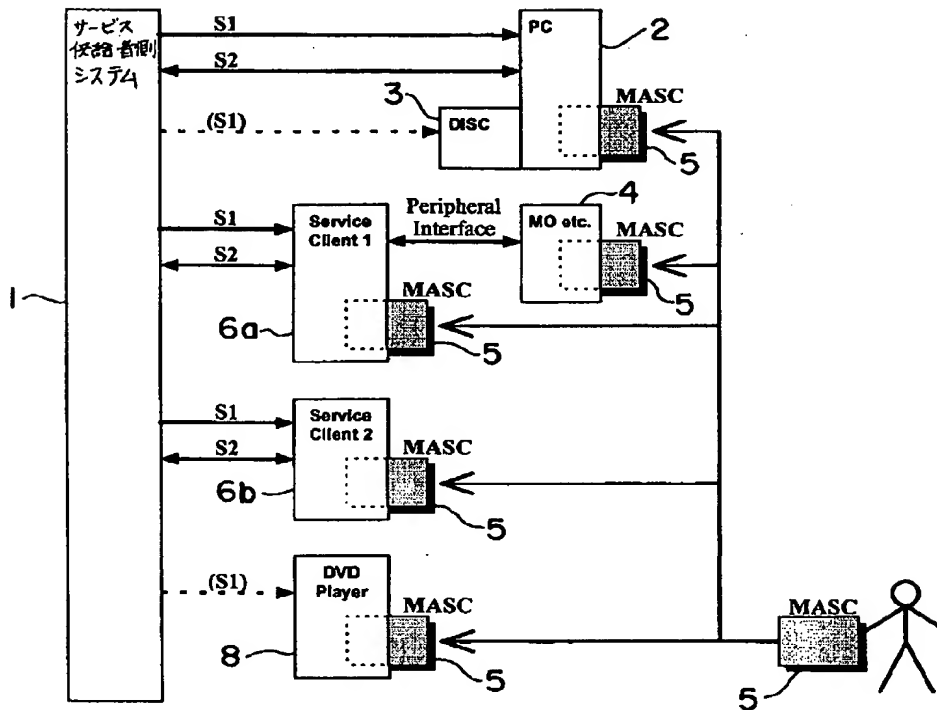
【図3】

図1のサービス提供者側システムの構成を示すブロック図



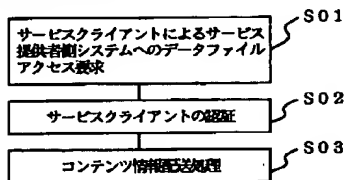
【図1】

本発明の一実施例によるクライアント認証システムが適用されたデジタル・オーディオ・インタラクティブ・システムの概略図



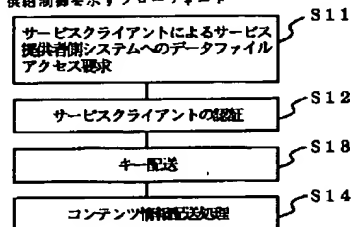
【図5】

秘密保持性が高い通信媒体によるコンテンツ情報供給制御を示すフローチャート



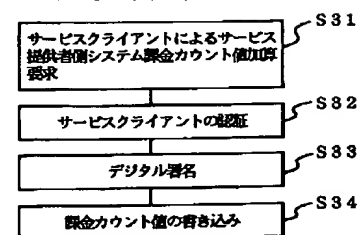
【図7】

一般のネットワークによるコンテンツ情報供給制御を示すフローチャート



【図12】

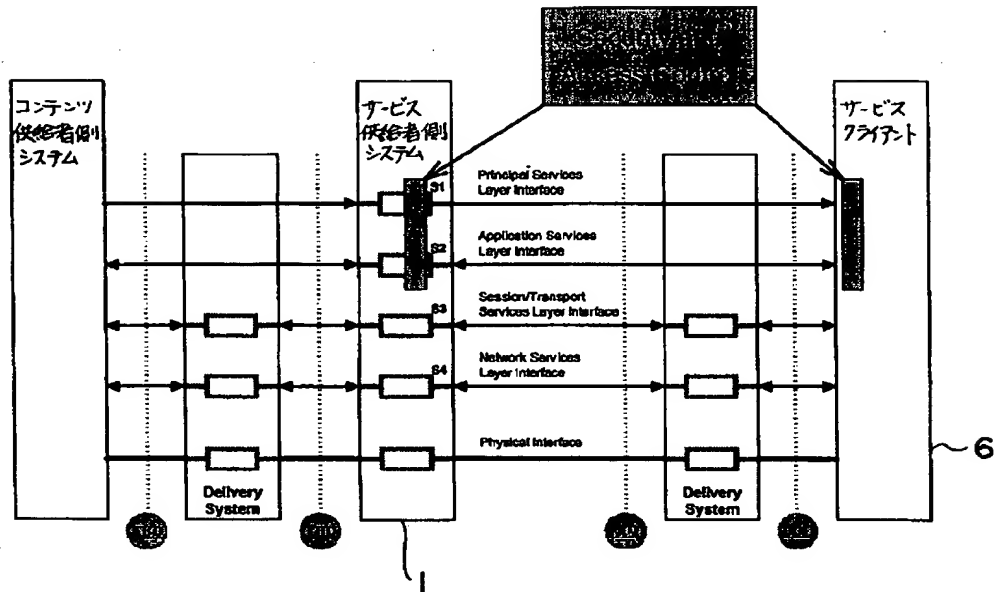
ローカル課金処理の内容を示すフローチャート





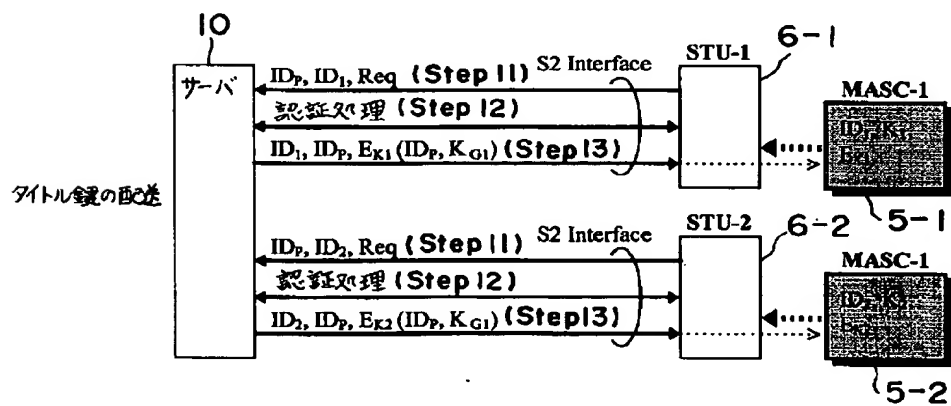
【図2】

図1のデジタル・オーディオ・インタラクティブ・システムに対応するシステムリファレンスモデルを示す図



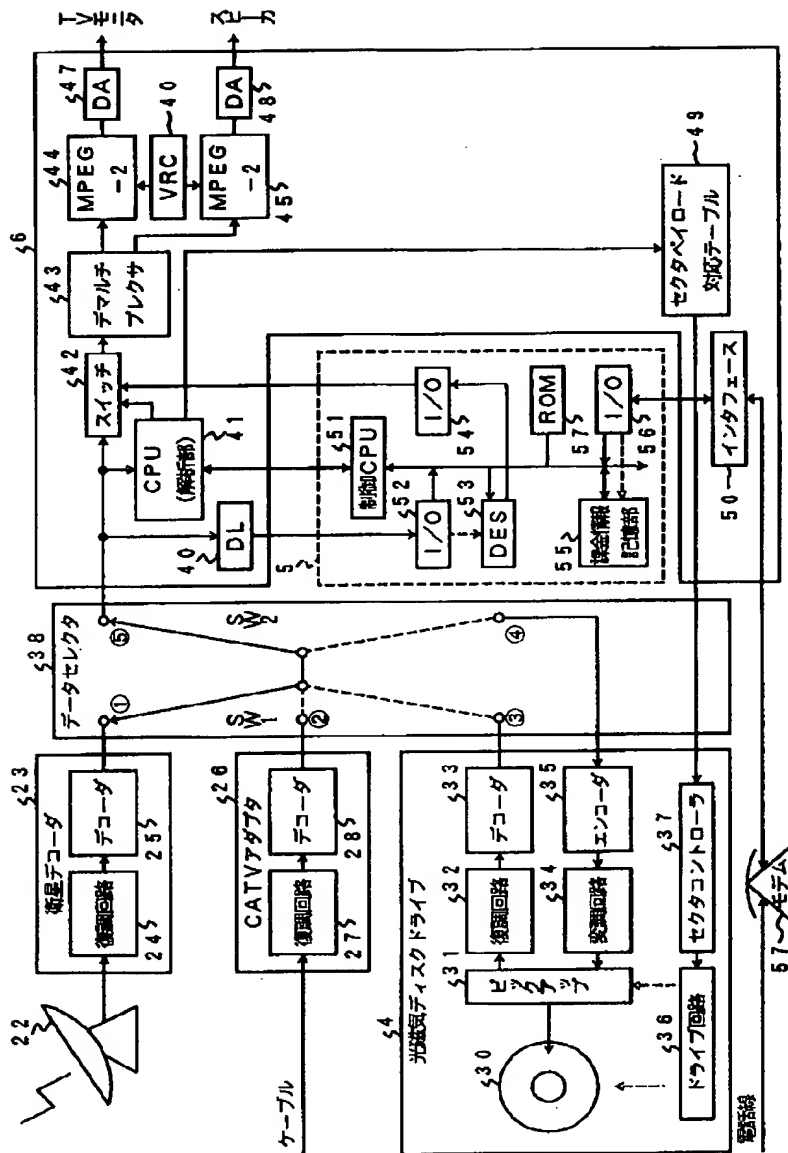
【図8】

鍵配送処理を示すタイムアロー図



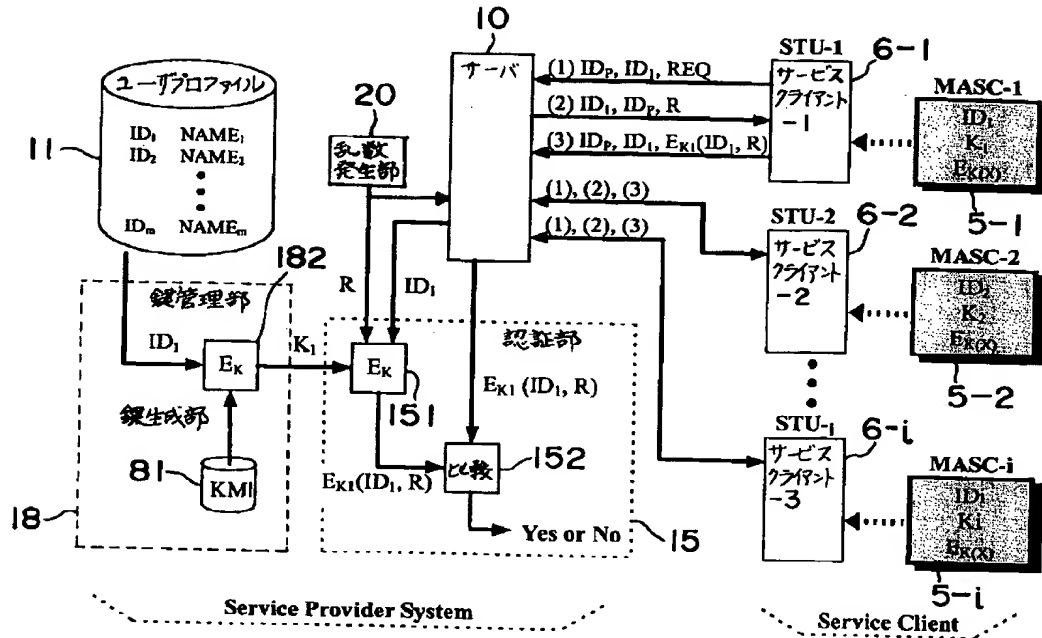
【図4】

図1のサービスライアント側システムの構成を示すブロック図



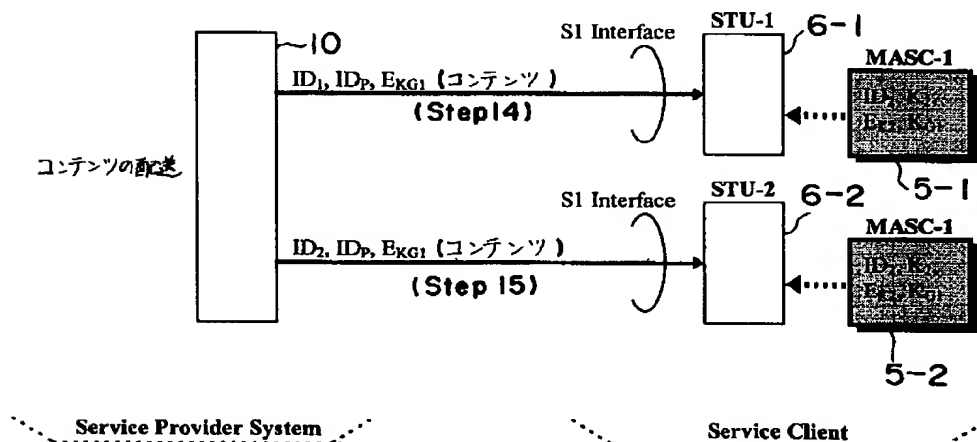
【図6】

認証処理に関連する構成を示すブロック図

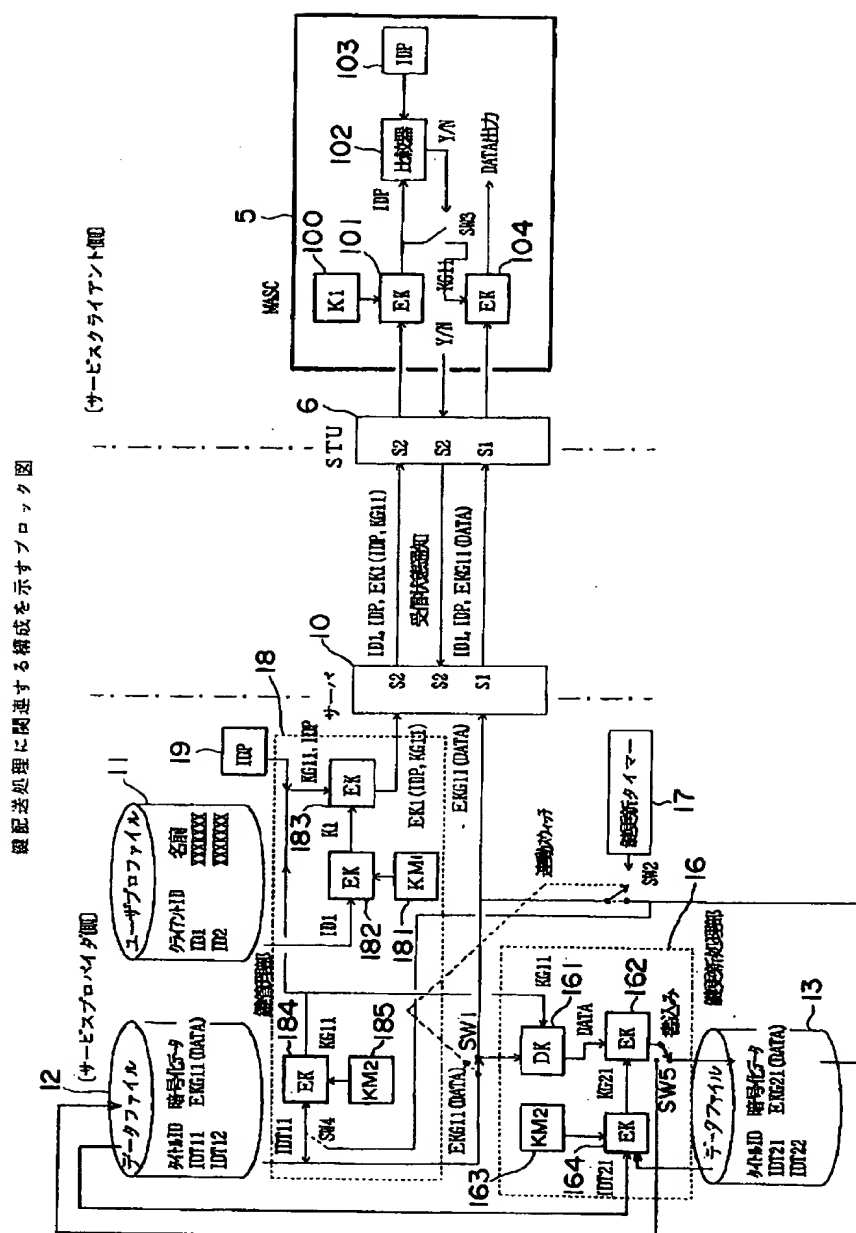


【図11】

コンテンツ配送処理を示すタイムアロー図

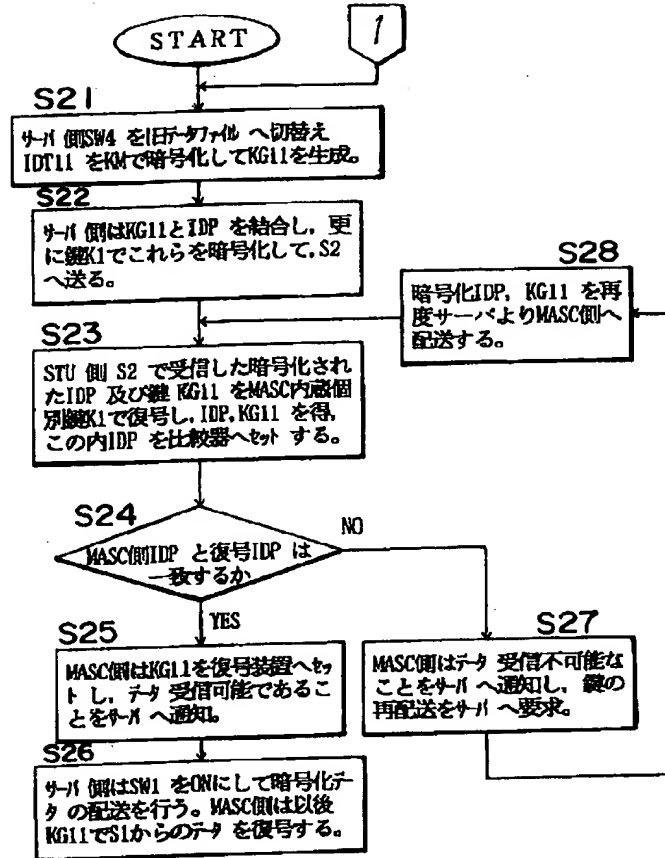


【図9】



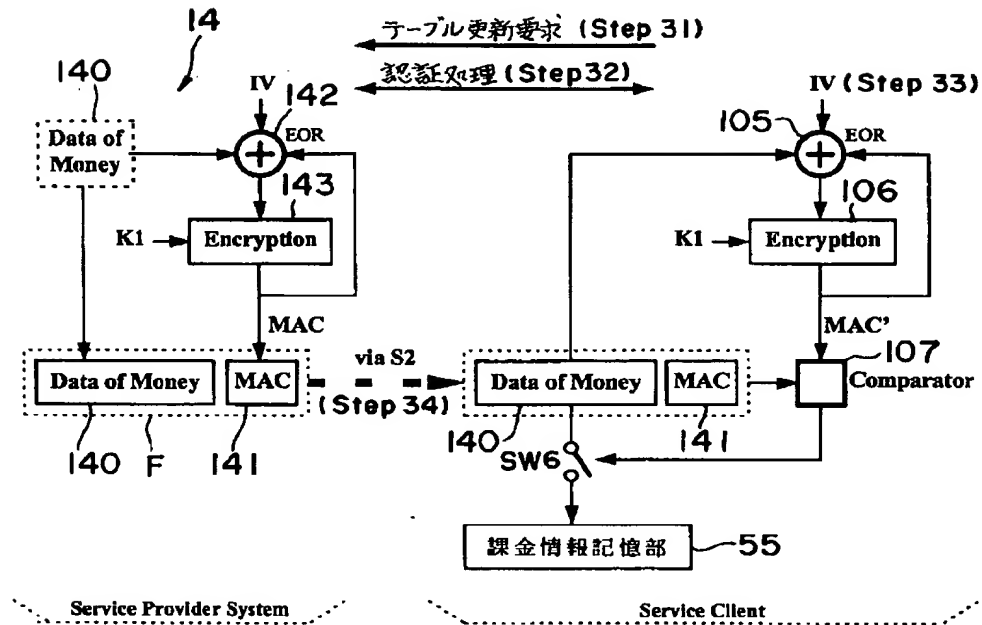
【図10】

鍵配送処理の内容を示すフローチャート



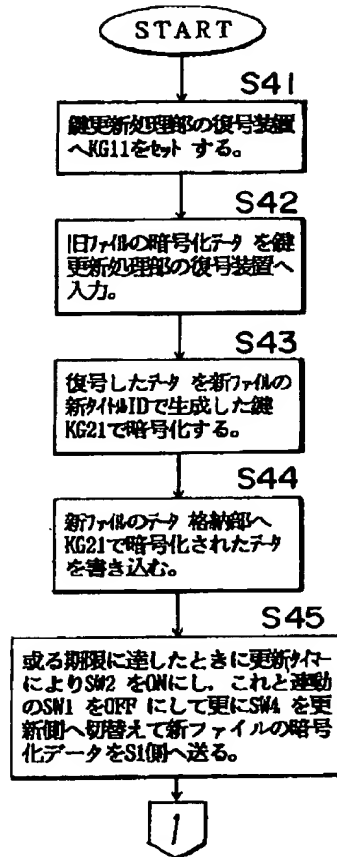
【図13】

デジタル署名処理に関連する構成を示すブロック図



【図14】

鍵の更新処理の内容を示すタイムアロー図



フロントページの続き

(72)発明者 古賀 譲  
神奈川県川崎市中原区上小田中1015番地  
富士通株式会社内

(72)発明者 石崎 正之  
神奈川県川崎市中原区上小田中1015番地  
富士通株式会社内